Further investigations on the QAM method for finding new APN functions

Nadiia Ichanska
(Joint work with Simon Berg and Nikolay S. Kaleyski)

University of Bergen

Selmer Seminar
March 18, 2024

Vectorial Boolean Functions and APN functions

$\mathbb{F}_{2^n}$ - finite field with 2^n elements, $n \in \mathbb{N}$.

- A function $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ is called **(n,n)**-function or **Vectorial Boolean Function**.

Vectorial Boolean Functions and APN functions

$\mathbb{F}_{2^n}$ - finite field with 2^n elements, $n \in \mathbb{N}$.

- A function $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ is called **(n,n)**-function or **Vectorial Boolean Function**.
- $F(x) = \sum_{i=0}^{2^n-1} a_i \cdot x^i, \; a_i \in \mathbb{F}_{2^n}$ - its **univariate representation.**

Vectorial Boolean Functions and APN functions

$\mathbb{F}_{2^n}$ - finite field with 2^n elements, $n \in \mathbb{N}$.

- A function $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ is called **(n,n)**-function or **Vectorial Boolean Function**.
- $F(x) = \sum_{i=0}^{2^n-1} a_i \cdot x^i,\ a_i \in \mathbb{F}_{2^n}$ - its **univariate representation.**
- $D_aF(x) = F(a+x) + F(x)$ - its **derivative** in the direction $a \in \mathbb{F}_{2^n} \setminus \{0\}$.

Vectorial Boolean Functions and APN functions

$\mathbb{F}_{2^n}$ - finite field with 2^n elements, $n \in \mathbb{N}$.

- A function $F : \mathbb{F}_{2^n} \rightarrow \mathbb{F}_{2^n}$ is called **(n,n)**-function or **Vectorial Boolean Function**.
- $F(x) = \sum_{i=0}^{2^n-1} a_i \cdot x^i, \; a_i \in \mathbb{F}_{2^n}$ - its **univariate representation.**
- $D_aF(x) = F(a+x) + F(x)$ - its **derivative** in the direction $a \in \mathbb{F}_{2^n} \setminus \{0\}$.
- $\Delta_aF(x) = F(a+x) + F(x) + F(a) + F(0)$ - **symmetric derivative** in the direction $a \in \mathbb{F}_{2^n} \setminus \{0\}$ of F.

Vectorial Boolean Functions and APN functions

$\mathbb{F}_{2^n}$ - finite field with 2^n elements, $n \in \mathbb{N}$.

- A function $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ is called **(n,n)**-function or **Vectorial Boolean Function**.
- $F(x) = \sum_{i=0}^{2^n-1} a_i \cdot x^i,\ a_i \in \mathbb{F}_{2^n}$ - its **univariate representation.**
- $\Delta_a F(x) = F(a+x) + F(x) + F(a) + F(0)$ - **symmetric derivative** in the direction $a \in \mathbb{F}_{2^n} \setminus \{0\}$ of F.

Vectorial Boolean Functions and APN functions

$\mathbb{F}_{2^n}$ - finite field with 2^n elements, $n \in \mathbb{N}$.

- A function $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ is called **(n,n)**-function or **Vectorial Boolean Function**.
- $F(x) = \sum_{i=0}^{2^n-1} a_i \cdot x^i, \; a_i \in \mathbb{F}_{2^n}$ - its **univariate representation.**
- $\Delta_a F(x) = F(a+x) + F(x) + F(a) + F(0)$ - **symmetric derivative** in the direction $a \in \mathbb{F}_{2^n} \setminus \{0\}$ of F.
- $\delta_F = \max_{a,b \in \mathbb{F}_{2^n}, a \neq 0} |\{x \in \mathbb{F}_{2^n} : \Delta_F(a,x) = b\}|$ - its **differential unifomity**.

Vectorial Boolean Functions and APN functions

$\mathbb{F}_{2^n}$ - finite field with 2^n elements, $n \in \mathbb{N}$.

- A function $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ is called **(n,n)**-function or **Vectorial Boolean Function**.
- $F(x) = \sum_{i=0}^{2^n-1} a_i \cdot x^i, \; a_i \in \mathbb{F}_{2^n}$ - its **univariate representation.**
- $\Delta_a F(x) = F(a+x) + F(x) + F(a) + F(0)$ - **symmetric derivative** in the direction $a \in \mathbb{F}_{2^n} \setminus \{0\}$ of F.
- $\delta_F = \max\limits_{a,b \in \mathbb{F}_{2^n}, a \neq 0} |\{x \in \mathbb{F}_{2^n} : \Delta_F(a,x) = b\}|$ - its **differential unifomity**.
- F is **almost perfect nonlinear(APN)** if $\delta_F = 2$.

- The **algebraic degree** of a function $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ is $\deg(F) = \max_{\substack{0 \le i \le 2^n-1 \\ a_i \neq 0}} w_2(i)$, where $w_2(i)$ is the 2-weight of the exponent i.

- The **algebraic degree** of a function $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ is $\deg(F) = \max_{\substack{0 \le i \le 2^n-1 \\ a_i \neq 0}} w_2(i)$, where $w_2(i)$ is the 2-weight of the exponent i.
- F is a **linear** function if $F(x) = \sum_{0 \le i < n} a_i x^{2^i}$, $a_i \in \mathbb{F}_{2^n}$.

  F is **affine** if it is a sum of a linear and a constant.

- The **algebraic degree** of a function $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ is $\deg(F) = \max\limits_{\substack{0 \le i \le 2^n-1 \\ a_i \neq 0}} w_2(i)$, where $w_2(i)$ is the 2-weight of the exponent i.
- F is a **linear** function if $F(x) = \sum\limits_{0 \le i < n} a_i x^{2^i}$, $a_i \in \mathbb{F}_{2^n}$.
  F is **affine** if it is a sum of a linear and a constant.
- F is **quadratic** if $\deg(F) \le 2$.

- The **algebraic degree** of a function $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ is $\deg(F) = \max_{\substack{0 \le i \le 2^n-1 \\ a_i \neq 0}} w_2(i)$, where $w_2(i)$ is the 2-weight of the exponent i.
- F is a **linear** function if $F(x) = \sum_{0 \le i < n} a_i x^{2^i}, \ a_i \in \mathbb{F}_{2^n}$.
  F is **affine** if it is a sum of a linear and a constant.
- F is **quadratic** if $\deg(F) \le 2$.
- We will consider homogeneous quadratic (n, n)-function F

$$F(x) = \sum_{0 \le i < j \le n-1} a_{i,j} x^{2^i + 2^j}, \ a_{i,j} \in \mathbb{F}_{2^n}.$$

Equivalence

The functions F and F' from $\mathbb{F}_{2^n}$ to itself are called

- affine equivalent (or linear equivalent) if $F' = A_1 \circ F \circ A_2$ for affine (linear) permutations A_1, A_2 from $\mathbb{F}_{2^n}$ to itself.

Equivalence

The functions F and F' from $\mathbb{F}_{2^n}$ to itself are called

- affine equivalent (or linear equivalent) if $F' = A_1 \circ F \circ A_2$ for affine (linear) permutations A_1, A_2 from $\mathbb{F}_{2^n}$ to itself.
- EA-equivalent if F' and $F + A$ are affine equivalent for affine mapping A.

Equivalence

The functions F and F' from $\mathbb{F}_{2^n}$ to itself are called

- affine equivalent (or linear equivalent) if $F' = A_1 \circ F \circ A_2$ for affine (linear) permutations A_1, A_2 from $\mathbb{F}_{2^n}$ to itself.
- EA-equivalent if F' and $F + A$ are affine equivalent for affine mapping A.
- Carlet-Charpin-Zinoviev(CCZ-equivalent).

Equivalence

The functions F and F' from $\mathbb{F}_{2^n}$ to itself are called

- affine equivalent (or linear equivalent) if $F' = A_1 \circ F \circ A_2$ for affine (linear) permutations A_1, A_2 from $\mathbb{F}_{2^n}$ to itself.
- EA-equivalent if F' and $F + A$ are affine equivalent for affine mapping A.
- Carlet-Charpin-Zinoviev(CCZ-equivalent).
  For quadratic APN (n, n) - functions, F and F' are CCZ-equivalent if and only if they are EA-equivalent [2].

QAM of the quadratic function over $\mathbb{F}_{2^n}$

- Let $F(x) = \sum_{0 \leq i < j \leq n-1} a_{i,j} x^{2^i + 2^j}$ over $\mathbb{F}_{2^n}$.

QAM of the quadratic function over $\mathbb{F}_{2^n}$

- Let $F(x) = \sum_{0 \le i < j \le n-1} a_{i,j} x^{2^i + 2^j}$ over $\mathbb{F}_{2^n}$.
- Let us set a normal basis $\mathcal{B} = \{b, b^2, \ldots, b^{2^{n-1}}\}$ of $\mathbb{F}_{2^n}$ over $\mathbb{F}_2$.

QAM of the quadratic function over $\mathbb{F}_{2^n}$

- Let $F(x) = \sum_{0 \le i < j \le n-1} a_{i,j} x^{2^i + 2^j}$ over $\mathbb{F}_{2^n}$.
- Let us set a normal basis $\mathcal{B} = \{b, b^2, \ldots, b^{2^{n-1}}\}$ of $\mathbb{F}_{2^n}$ over $\mathbb{F}_2$.
- [3] The **rank** of the vector $v \in \mathbb{F}_{2^n}^n$ is the dimension of the subspace spanned by its elements.

QAM of the quadratic function over $\mathbb{F}_{2^n}$

- Let $F(x) = \sum_{0 \le i < j \le n-1} a_{i,j} x^{2^i + 2^j}$ over $\mathbb{F}_{2^n}$.
- Let us set a normal basis $\mathcal{B} = \{b, b^2, \ldots, b^{2^{n-1}}\}$ of $\mathbb{F}_{2^n}$ over $\mathbb{F}_2$.
- [3] The **rank** of the vector $v \in \mathbb{F}_{2^n}^n$ is the dimension of the subspace spanned by its elements.
- The **derivative matrix** $M_F \in \mathbb{F}_{2^n}^{n \times n}$ of function F is

$$M_F = \begin{bmatrix} \Delta_b F(b) & \Delta_b F(b^2) & \ldots & \Delta_b F(b^n) \\ \Delta_{b^2} F(b) & \Delta_{b^2} F(b^2) & \ldots & \Delta_{b^2} F(b^n) \\ \vdots & \vdots & \ddots & \vdots \\ \Delta_{b^n} F(b) & \Delta_{b^n} F(b^2) & \ldots & \Delta_{b^n} F(b^n) \end{bmatrix}.$$

QAM of the quadratic function over $\mathbb{F}_{2^n}$

- The **derivative matrix** $M_F \in \mathbb{F}_{2^n}^{n \times n}$ of function F is

$$M_F = \begin{bmatrix} \Delta F(b, b) & \Delta F(b, b^2) & \dots & \Delta F\left(b, b^n\right) \\ \Delta F(b, b^2) & \Delta F(b^2, b^2) & \dots & \Delta F\left(b^2, b^n\right) \\ \vdots & \vdots & \ddots & \vdots \\ \Delta F\left(b, b^n\right) & \Delta F\left(b^2, b^n\right) & \dots & \Delta F\left(b^n, b^n\right) \end{bmatrix}. \tag{1}$$

QAM of the quadratic function over $\mathbb{F}_{2^n}$

- The **derivative matrix** $M_F \in \mathbb{F}_{2^n}^{n\times n}$ of function F is

$$M_F = \begin{bmatrix} \Delta F(b,b) & \Delta F(b,b^2) & \dots & \Delta F(b,b^n) \\ \Delta F(b,b^2) & \Delta F(b^2,b^2) & \dots & \Delta F(b^2,b^n) \\ \vdots & \vdots & \ddots & \vdots \\ \Delta F(b,b^n) & \Delta F(b^2,b^n) & \dots & \Delta F(b^n,b^n) \end{bmatrix}. \tag{1}$$

- A matrix $M_F \in \mathbb{F}_{2^n}^{n\times n}$ is called a **Quadratic APN Matrix (QAM)** [3] if:

QAM of the quadratic function over $\mathbb{F}_{2^n}$

- The **derivative matrix** $M_F \in \mathbb{F}_{2^n}^{n\times n}$ of function F is

$$M_F = \begin{bmatrix} \Delta F(b,b) & \Delta F(b,b^2) & \dots & \Delta F\left(b,b^n\right) \\ \Delta F(b,b^2) & \Delta F(b^2,b^2) & \dots & \Delta F\left(b^2,b^n\right) \\ \vdots & \vdots & \ddots & \vdots \\ \Delta F\left(b,b^n\right) & \Delta F\left(b^2,b^n\right) & \dots & \Delta F\left(b^n,b^n\right) \end{bmatrix}. \tag{1}$$

- A matrix $M_F \in \mathbb{F}_{2^n}^{n\times n}$ is called a **Quadratic APN Matrix (QAM)** [3] if:
  1. M_F is symmetric and the elements in its main diagonal are all zeros;

QAM of the quadratic function over $\mathbb{F}_{2^n}$

- The **derivative matrix** $M_F \in \mathbb{F}_{2^n}^{n \times n}$ of function F is

$$M_F = \begin{bmatrix} \Delta F(b,b) & \Delta F(b,b^2) & \dots & \Delta F\left(b,b^n\right) \\ \Delta F(b,b^2) & \Delta F(b^2,b^2) & \dots & \Delta F\left(b^2,b^n\right) \\ \vdots & \vdots & \ddots & \vdots \\ \Delta F\left(b,b^n\right) & \Delta F\left(b^2,b^n\right) & \dots & \Delta F\left(b^n,b^n\right) \end{bmatrix}. \tag{1}$$

- A matrix $M_F \in \mathbb{F}_{2^n}^{n \times n}$ is called a **Quadratic APN Matrix (QAM)** [3] if:
  1. M_F is symmetric and the elements in its main diagonal are all zeros;
  2. Every nonzero linear combination of the n rows (or columns, since M_F is symmetric) of M_F has rank $n-1$.

Following Corollary 5 from [1], we get that function

$$F(x) = \sum_{0 \le i < j \le n-1} a_{i,j} x^{2^i + 2^j}, \; a_{i,j} \in \mathbb{F}_{2^n} \tag{2}$$

is APN if and only if its derivative matrix M_F is QAM.

Structure of the derivative matrix (1)

- Let $F(x) = \sum_{0 \leq i < j \leq n-1} a_{i,j} x^{2^i + 2^j}$ with coefficients $a_{i,j} \in \mathbb{F}_{2^m}$ in some subfield $\mathbb{F}_{2^m}$ of $\mathbb{F}_{2^n}$

Structure of the derivative matrix (1)

- Let $F(x) = \sum_{0 \leq i < j \leq n-1} a_{i,j} x^{2^i + 2^j}$ with coefficients $a_{i,j} \in \mathbb{F}_{2^m}$ in some subfield $\mathbb{F}_{2^m}$ of $\mathbb{F}_{2^n}$
- $(F(x))^{2^m} = a_i^{2^m} \left(x^i\right)^{2^m} = \sum_{i=0}^{2^n-1} a_i \left(x^i\right)^{2^m} = F\left(x^{2^m}\right),$

Structure of the derivative matrix (1)

- Let $F(x) = \sum_{0 \leq i < j \leq n-1} a_{i,j} x^{2^i + 2^j}$ with coefficients $a_{i,j} \in \mathbb{F}_{2^m}$ in some subfield $\mathbb{F}_{2^m}$ of $\mathbb{F}_{2^n}$
- $(F(x))^{2^m} = a_i^{2^m} \left(x^i\right)^{2^m} = \sum_{i=0}^{2^n-1} a_i \left(x^i\right)^{2^m} = F\left(x^{2^m}\right)$,
- $(\Delta_a F(x))^{2^m} = F(x+a)^{2^m} + F(x)^{2^m} + F(a)^{2^m} = \Delta_{a^{2^m}} F\left(x^{2^m}\right)$,

Structure of the derivative matrix (1)

- Let $F(x) = \sum_{0 \le i < j \le n-1} a_{i,j} x^{2^i + 2^j}$ with coefficients $a_{i,j} \in \mathbb{F}_{2^m}$ in some subfield $\mathbb{F}_{2^m}$ of $\mathbb{F}_{2^n}$
- $(F(x))^{2^m} = a_i^{2^m} \left(x^i\right)^{2^m} = \sum_{i=0}^{2^n-1} a_i \left(x^i\right)^{2^m} = F\left(x^{2^m}\right)$,
- $(\Delta_a F(x))^{2^m} = F(x+a)^{2^m} + F(x)^{2^m} + F(a)^{2^m} = \Delta_{a^{2^m}} F\left(x^{2^m}\right)$,

$$M_{i+m,j+m} = (M_{i,j})^{2^m}.$$

Structure of the derivative matrix (1)

- Let $F(x) = \sum_{0 \leq i < j \leq n-1} a_{i,j} x^{2^i + 2^j}$ with coefficients $a_{i,j} \in \mathbb{F}_{2^m}$ in some subfield $\mathbb{F}_{2^m}$ of $\mathbb{F}_{2^n}$
- $(F(x))^{2^m} = a_i^{2^m} \left(x^i\right)^{2^m} = \sum_{i=0}^{2^n-1} a_i \left(x^i\right)^{2^m} = F\left(x^{2^m}\right)$,
- $(\Delta_a F(x))^{2^m} = F(x+a)^{2^m} + F(x)^{2^m} + F(a)^{2^m} = \Delta_{a^{2^m}} F\left(x^{2^m}\right)$,

$$M_{i+m,j+m} = (M_{i,j})^{2^m}.$$

$$\begin{bmatrix} 0 & \Delta F(b_1, b_2) & \dots & \dots & \Delta F(b_1, b_n) \\ \Delta F(b_1, b_2) & 0 & \ddots & \dots & \Delta F(b_2, b_n) \\ \vdots & \ddots & \ddots & (\Delta F(b_1, b_2))^{2^m} & \vdots \\ \vdots & \ddots & (\Delta F(b_1, b_2))^{2^m} & 0 & \vdots \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ \Delta F(b_1, b_n) & \Delta F(b_2, b_n) & \dots & \dots & 0 \end{bmatrix}$$

Structure of the search

$$M_F = \begin{pmatrix} 0 & \Omega_1 & \Omega_2 & \dots & \dots & \dots \\ \Omega_1 & 0 & \ddots & \ddots & \dots & \dots \\ \Omega_2 & \dots & 0 & \Omega_1^{2^m} & \Omega_2^{2^m} & \dots \\ \vdots & \vdots & \Omega_1^{2^m} & 0 & \dots & \dots \\ \vdots & \vdots & \Omega_2^{2^m} & \dots & 0 & \dots \\ \vdots & \vdots & \vdots & \vdots & \vdots & \ddots \end{pmatrix}, \tag{3}$$

where $\Omega_1, \Omega_2, \dots, \Omega_l \in \mathbb{F}_{2^n}$ - **variables**.

Structure of the search

$$M_F = \begin{pmatrix} 0 & \Omega_1 & \Omega_2 & \dots & \dots & \dots \\ \Omega_1 & 0 & \ddots & \ddots & \dots & \dots \\ \Omega_2 & \dots & 0 & \Omega_1^{2^m} & \Omega_2^{2^m} & \dots \\ \vdots & \vdots & \Omega_1^{2^m} & 0 & \dots & \dots \\ \vdots & \vdots & \Omega_2^{2^m} & \dots & 0 & \dots \\ \vdots & \vdots & \vdots & \vdots & \vdots & \ddots \end{pmatrix}, \tag{3}$$

where $\Omega_1, \Omega_2, \dots, \Omega_l \in \mathbb{F}_{2^n}$ - **variables**.
A variable Ω_i is located on the i-th **level**.

Orbit restrictions

Theorem 3 [3]

For any linear permutation l on $\mathbb{F}_{2^n}$ and $M \in \mathbb{F}_{2^n}^{n \times n}$ s.t. $M = M_F$ then any $M' = M_{F'}$ produced by

$$M'_{i,j} = l(M_{i,j}) \text{ for all } 1 \leq i, j \leq n \tag{4}$$

will be $F' = l \circ F$ linearly equivalent(also EA-equivalent) to F.

Orbit restrictions

Theorem 3 [3]

For any linear permutation l on $\mathbb{F}_{2^n}$ and $M \in \mathbb{F}_{2^n}^{n\times n}$ s.t. $M = M_F$ then any $M' = M_{F'}$ produced by

$$M'_{i,j} = l(M_{i,j}) \text{ for all } 1 \leq i,j \leq n \tag{4}$$

will be $F' = l \circ F$ linearly equivalent(also EA-equivalent) to F.

Let $\mathcal{L}$ be a set of all linear (n,n)-permutations $l = \sum_{i=1}^{n} \alpha_i x^{2^{i-1}}$ on $\mathbb{F}_{2^n}$ with subfield $\alpha_i \in \mathbb{F}_{2^m}$.

Orbit restrictions

Theorem 3 [3]

For any linear permutation l on $\mathbb{F}_{2^n}$ and $M \in \mathbb{F}_{2^n}^{n\times n}$ s.t. $M = M_F$ then any $M' = M_{F'}$ produced by

$$M'_{i,j} = l(M_{i,j}) \text{ for all } 1 \leq i,j \leq n \tag{4}$$

will be $F' = l \circ F$ linearly equivalent(also EA-equivalent) to F.

Let $\mathcal{L}$ be a set of all linear (n,n)-permutations $l = \sum_{i=1}^{n} \alpha_i x^{2^{i-1}}$ on $\mathbb{F}_{2^n}$ with subfield $\alpha_i \in \mathbb{F}_{2^m}$. Then the **orbit** of $a \in \mathbb{F}_{2^n}$

$$Orb(a,\mathcal{L}) = \{l(a) : l \in \mathcal{L}\}. \tag{5}$$

Orbit Restrictions

$$\mathbb{F}_{2^n} = Orb(a_1, \mathcal{L}) \cup \cdots \cup Orb(a_k, \mathcal{L}), \text{ for some } a_i \in \mathbb{F}_{2^n},\ 1 \leq i \leq k.$$

Orbit Restrictions

$$\mathbb{F}_{2^n} = Orb(a_1, \mathcal{L}) \cup \cdots \cup Orb(a_k, \mathcal{L}),\ \text{for some } a_i \in \mathbb{F}_{2^n},\ 1 \leq i \leq k.$$

$$M_{F'} = \begin{pmatrix} 0 & L(\Omega_1) & L(\Omega_2) & \dots & \dots & \dots \\ L(\Omega_1) & 0 & \ddots & \ddots & \dots & \dots \\ L(\Omega_2) & \dots & 0 & L(\Omega_1^{2^m}) & L(\Omega_2^{2^m}) & \dots \\ \vdots & \vdots & L(\Omega_1^{2^m}) & 0 & \dots & \dots \\ \vdots & \vdots & L(\Omega_2^{2^m}) & \dots & 0 & \dots \\ \vdots & \vdots & \vdots & \vdots & \vdots & \ddots \end{pmatrix},$$

where $L(\Omega_i^{2^{m*j}}) = (L(\Omega_i))^{2^{m*j}}$, $j \in \{1, \dots, n/m - 1\}$ for any variable Ω_i, $1 \leq i \leq l$.

Orbit partition level by level

$$\mathbb{F}_{2^n} = Orb(A, \mathcal{L}) \cup \ldots, \; A \in \mathbb{F}_{2^n}.$$

Orbit partition level by level

$$\mathbb{F}_{2^n} = Orb(A, \mathcal{L}) \cup \dots, \; A \in \mathbb{F}_{2^n}.$$

$$M_F = \begin{pmatrix} 0 & A & \Omega_2 & \dots & \dots & \dots \\ A & 0 & \ddots & \ddots & \dots & \dots \\ \Omega_2 & \dots & 0 & A^{2^m} & \Omega_2^{2^m} & \dots \\ \vdots & \vdots & A^{2^m} & 0 & \dots & \dots \\ \vdots & \vdots & \Omega_2^{2^m} & \dots & 0 & \dots \\ \vdots & \vdots & \vdots & \vdots & \vdots & \ddots \end{pmatrix}.$$

Orbit partition level by level

$$\mathbb{F}_{2^n} = Orb(A, \mathcal{L}) \cup \ldots, \; A \in \mathbb{F}_{2^n}.$$

$$M_F = \begin{pmatrix} 0 & A & \Omega_2 & \ldots & \ldots & \ldots \\ A & 0 & \ddots & \ddots & \ldots & \ldots \\ \Omega_2 & \ldots & 0 & A^{2^m} & \Omega_2^{2^m} & \ldots \\ \vdots & \vdots & A^{2^m} & 0 & \ldots & \ldots \\ \vdots & \vdots & \Omega_2^{2^m} & \ldots & 0 & \ldots \\ \vdots & \vdots & \vdots & \vdots & \vdots & \ddots \end{pmatrix}.$$

$$Orb_A(\Omega_2, \mathcal{L}) = \{I(\Omega_2) : I \in \mathcal{L} \mid I(A) = A\}.$$

Orbit partition level by level

$$\mathbb{F}_{2^n} = Orb(A, \mathcal{L}) \cup \ldots, \; A \in \mathbb{F}_{2^n}.$$

$$M_F = \begin{pmatrix} 0 & A & \Omega_2 & \ldots & \ldots & \ldots \\ A & 0 & \ddots & \ddots & \ldots & \ldots \\ \Omega_2 & \ldots & 0 & A^{2^m} & \Omega_2^{2^m} & \ldots \\ \vdots & \vdots & A^{2^m} & 0 & \ldots & \ldots \\ \vdots & \vdots & \Omega_2^{2^m} & \ldots & 0 & \ldots \\ \vdots & \vdots & \vdots & \vdots & \vdots & \ddots \end{pmatrix}.$$

$$Orb_A(\Omega_2, \mathcal{L}) = \{l(\Omega_2) : l \in \mathcal{L} \mid l(A) = A\}.$$

$$S = \{\Omega_1, \ldots, \Omega_{k-1}\}$$

$$Orb_S(\Omega_k, \mathcal{L}) = \{l(\Omega_k) : l \in \mathcal{L} \mid \forall X \in S : \; l(X) = X\}.$$

Submatrix method

- Let $M \in \mathbb{F}_{2^n}^{n \times n}$ be a derivative matrix.

Submatrix method

- Let $M \in \mathbb{F}_{2^n}^{n \times n}$ be a derivative matrix.
- M is QAM if and only if every submatrix $S \in \mathbb{F}_{2^n}^{p \times q}$, $1 \leq p, q \leq n$ of M is **proper**.

Submatrix method

- Let $M \in \mathbb{F}_{2^n}^{n \times n}$ be a derivative matrix.
- M is QAM if and only if every submatrix $S \in \mathbb{F}_{2^n}^{p \times q}$, $1 \leq p, q \leq n$ of M is **proper**.
- S **proper** if every nonzero linear combinations of the p rows has rank at least $q - 1$.

Submatrix method

- Let $M \in \mathbb{F}_{2^n}^{n\times n}$ be a derivative matrix.
- M is QAM if and only if every submatrix $S \in \mathbb{F}_{2^n}^{p\times q}$, $1 \leq p, q \leq n$ of M is **proper**.
- $$\begin{pmatrix} 0 & A & B & \Omega_3 & \dots & \dots \\ A & 0 & \ddots & \ddots & \dots & \dots \\ B & \dots & 0 & A^{2^m} & B^{2^m} & \dots \\ \Omega_3 & \vdots & A^{2^m} & 0 & \dots & \dots \\ \vdots & \vdots & B^{2^m} & \dots & 0 & \dots \end{pmatrix}.$$

Submatrix method

- Let $M \in \mathbb{F}_{2^n}^{n \times n}$ be a derivative matrix.
- M is QAM if and only if every submatrix $S \in \mathbb{F}_{2^n}^{p \times q}$, $1 \leq p, q \leq n$ of M is **proper**.
- $$\begin{pmatrix} 0 & A & B & \Omega_3 & \dots & \dots \\ A & 0 & \ddots & \ddots & \dots & \dots \\ B & \dots & 0 & A^{2^m} & B^{2^m} & \dots \\ \Omega_3 & \vdots & A^{2^m} & 0 & \dots & \dots \\ \vdots & \vdots & B^{2^m} & \dots & 0 & \dots \end{pmatrix}.$$
- After considering $F' = F \circ L$, where $L = a_j x^{2^i}$, $a_j \in \mathbb{F}_{2^m}$, we could eliminate the number of submatrices for this test.

(8,2)

- $F(x)$ over $\mathbb{F}_{2^8}$ with coefficients in $\mathbb{F}_{2^2}$.

(8,2)

- $F(x)$ over $\mathbb{F}_{2^8}$ with coefficients in $\mathbb{F}_{2^2}$.
- $4^8 = 65536$ linear permutations with coefficients in the subfield were constructed.

(8,2)

- $F(x)$ over $\mathbb{F}_{2^8}$ with coefficients in $\mathbb{F}_{2^2}$.
- $4^8 = 65536$ linear permutations with coefficients in the subfield were constructed.
- By using these permutations, the first level of the search was partitioned into 4 orbits.

(8,2)

- $F(x)$ over $\mathbb{F}_{2^8}$ with coefficients in $\mathbb{F}_{2^2}$.
- $4^8 = 65536$ linear permutations with coefficients in the subfield were constructed.
- By using these permutations, the first level of the search was partitioned into 4 orbits.

1	a	a^7	a^{17}

Table: The first level

(8,2)

- $F(x)$ over $\mathbb{F}_{2^8}$ with coefficients in $\mathbb{F}_{2^2}$.
- $4^8 = 65536$ linear permutations with coefficients in the subfield were constructed.
- The number of variables = levels in this dimension is 8.
- By using these permutations, the first level of the search was partitioned into 4 orbit representatives.

1	a	a^7	a^{17}
$\#\{\Omega_2\}_i = 8$ $Orb_1\Omega_2$	$\#\{\Omega_2\}_i = 30$ $Orb_a\Omega_2$	$\#\{\Omega_2\}_i = 22$ $Orb_{a^7}\Omega_2$	$\#\{\Omega_2\}_i = 14$ $Orb_{a^{17}}\Omega_2$

Table: The second level

(8,2)

- $F(x)$ over $\mathbb{F}_{2^8}$ with coefficients in $\mathbb{F}_{2^2}$.

1	a	a^7	a^{17}
40 hours	1 month	10 days	7 days

(8,2)

- $F(x)$ over $\mathbb{F}_{2^8}$ with coefficients in $\mathbb{F}_{2^2}$.

1	a	a^7	a^{17}
40 hours	1 month	10 days	7 days

- 196863 quadratic APN functions were found in the search, with 27 unique ortho-derivative differential spectra.

(8,2)

- $F(x)$ over $\mathbb{F}_{2^8}$ with coefficients in $\mathbb{F}_{2^2}$.

1	a	a^7	a^{17}
40 hours	1 month	10 days	7 days

- 196863 quadratic APN functions were found in the search, with 27 unique ortho-derivative differential spectra.
- $\mathbf{a^{85}x^{96} + a^{85}x^{72} + a^{170}x^{24} + x^{18} + a^{85}x^{12} + a^{85}x^{9} + x^{6} + x^{3}}$.

(8,2)

- $F(x)$ over $\mathbb{F}_{2^8}$ with coefficients in $\mathbb{F}_{2^2}$.

1	a	a^7	a^{17}
40 hours	1 month	10 days	7 days

- 196863 quadratic APN functions were found in the search, with 27 unique ortho-derivative differential spectra.
- $\mathbf{a^{85}x^{96} + a^{85}x^{72} + a^{170}x^{24} + x^{18} + a^{85}x^{12} + a^{85}x^{9} + x^{6} + x^{3}}$.
- $\mathbf{0^{38196}, 2^{22008}, 4^{4608}, 6^{456}, 8^{12}}$ - its ortho-derivative differential spectra.

(10,2)

- $F(x)$ over $\mathbb{F}_{2^{10}}$ with coefficients in $\mathbb{F}_{2^2}$.
- $4^{10} = 1048576$ linear permutations with coefficients in the subfield were constructed.
- The number of variables = levels in this dimension is 9.
- By using these permutations, the first level of the search was partitioned into 3 orbit representatives.

1	a	a^5
$\#\{\Omega_2\}_i = 5$ $Orb_1\Omega_2$	$\#\{\Omega_2\}_i = 33$ $Orb_a\Omega_2$	$\#\{\Omega_2\}_i = 50$ $Orb_{a^5}\Omega_2$

(10,1)

- $F(x)$ over $\mathbb{F}_{2^{10}}$ with coefficients in $\mathbb{F}_{2^1}$.
- $2^{10} = 1024$ linear permutations with coefficients in the subfield were constructed.
- The number of variables = levels in this dimension is 5.
- By using these permutations, the first level of the search was partitioned into 8 orbit representatives.

1	a	a^5	a^{15}	a^{33}	a^{57}	a^{99}	a^{341}
# of orbit representatives for 2nd level after Sub-matrix Test							
0	746	1012	753	71	112	78	8

(9,3)

- $F(x)$ over $\mathbb{F}_{2^9}$ with coefficients in $\mathbb{F}_{2^3}$.
- $8^9 = 134217728$ linear permutations with coefficients in the subfield were constructed.
- The number of variables = levels in this dimension is 12.

(9,3)

- $F(x)$ over $\mathbb{F}_{2^9}$ with coefficients in $\mathbb{F}_{2^3}$.
- $8^9 = 134217728$ linear permutations with coefficients in the subfield were constructed.
- The number of variables = levels in this dimension is 12.

Remark

Let $a \in \mathbb{F}_{2^9}$. We categorize a into the following cases:

1. $Cat_1 = \{a : a \in \mathbb{F}_{2^9} \mid a + a^{2^3} = 0\}$,
2. $Cat_2 = \{a : a \in \mathbb{F}_{2^9} \mid a + a^{2^3} + a^{2^6} = 0\}$,
3. $Cat_3 = \{a : a \in \mathbb{F}_{2^9} \mid a \notin Cat_1,\ a \notin Cat_2\}$,

(9,3)

- $F(x)$ over $\mathbb{F}_{2^9}$ with coefficients in $\mathbb{F}_{2^3}$.
- $8^9 = 134217728$ linear permutations with coefficients in the subfield were constructed.
- The number of variables = levels in this dimension is 12.

Remark

Let $a \in \mathbb{F}_{2^9}$. We categorize a into the following cases:

1. $Cat_1 = \{a : a \in \mathbb{F}_{2^9} \mid a + a^{2^3} = 0\}$,
2. $Cat_2 = \{a : a \in \mathbb{F}_{2^9} \mid a + a^{2^3} + a^{2^6} = 0\}$,
3. $Cat_3 = \{a : a \in \mathbb{F}_{2^9} \mid a \notin Cat_1,\ a \notin Cat_2\}$,

Theorem

Let $a, b \in Cat_3$. If there exist $l(x) = \sum_{i=0}^{8} c_i x^{2^i},\ c_i \in \mathbb{F}_{2^3}$ s.t. $l(a) = b,\ l(a^{2^3}) = b^{2^3},\ l(a^{2^6}) = b^{2^6}$. Then there exist linear permutation $L \in \mathcal{L}$ s.t. $L(a) = b$.

Conclusions

- For $F(x)$ over $\mathbb{F}_{2^n}$ with coefficients in $\mathbb{F}_{2^m}$ we run searches (n, m) for $(8, 2), (10, 2), (10, 1), (9, 3)$.

Conclusions

- For $F(x)$ over $\mathbb{F}_{2^n}$ with coefficients in $\mathbb{F}_{2^m}$ we run searches (n, m) for $(8, 2), (10, 2), (10, 1), (9, 3)$.
- We conclude where it is feasible to get the results and improve the computational method as possible.

Conclusions

- For $F(x)$ over $\mathbb{F}_{2^n}$ with coefficients in $\mathbb{F}_{2^m}$ we run searches (n, m) for $(8, 2), (10, 2), (10, 1), (9, 3)$.
- We conclude where it is feasible to get the results and improve the computational method as possible.
- Computational searches are still running.

Diana Davidova and Nikolay Kaleyski.
Classification of all do planar polynomials with prime field coefficients over $gf(3^n)$ for n up to 7.
Cryptology ePrint Archive, Paper 2022/1059, 2022.
https://eprint.iacr.org/2022/1059.

Satoshi Yoshiara.
Equivalences of quadratic APN functions.
Journal of Algebraic Combinatorics, 35(3):461–475, 2012.

Yuyin Yu, Mingsheng Wang, and Yongqiang Li.
A matrix approach for constructing quadratic APN functions.
Designs, codes and cryptography, 73(2):587–600, 2014.